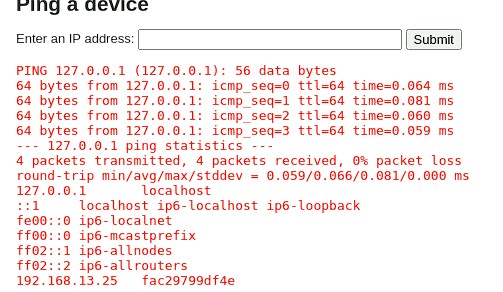
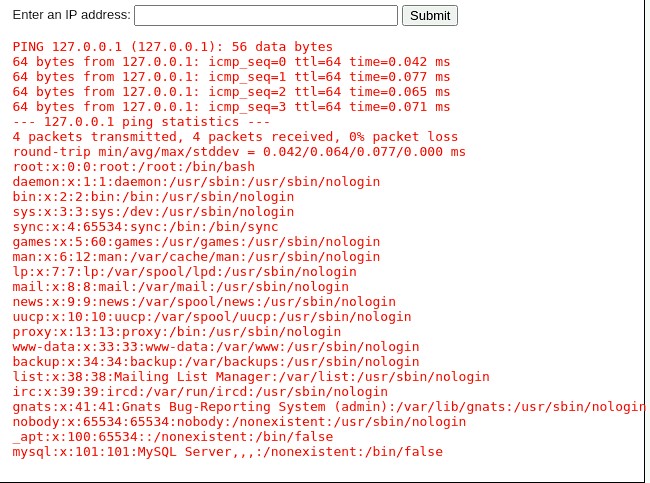
| Cybersecurity |
| --- |
| Module 15 Challenge Submission File |

## Testing Web Applications for Vulnerabilities

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

### Web Application 1: *Your Wish is My Command Injection*

Provide a screenshot confirming that you successfully completed this exploit:

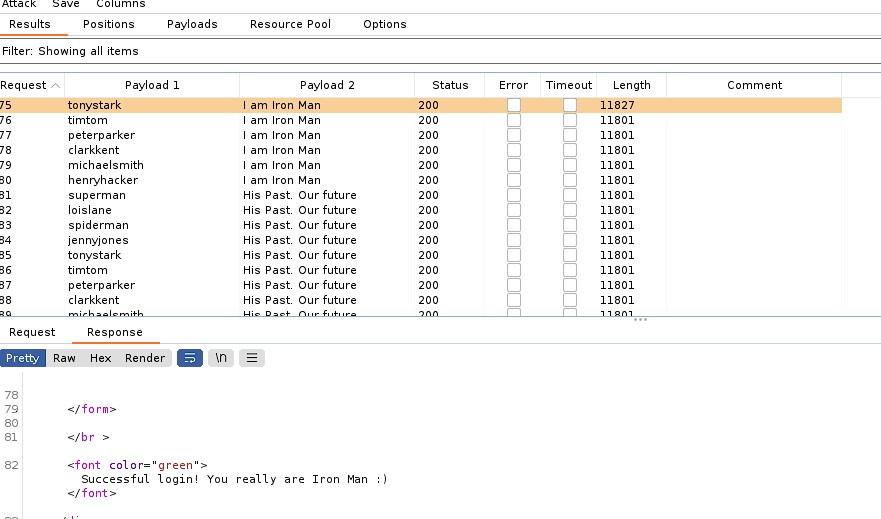
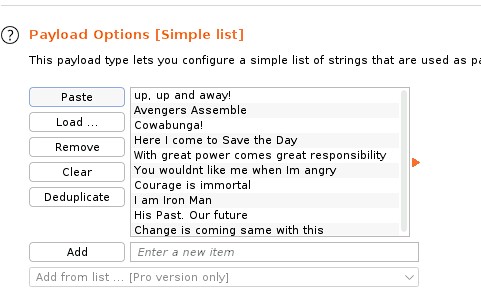
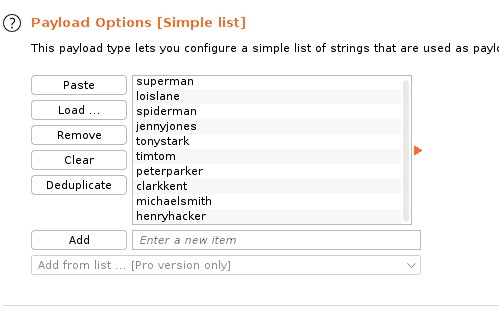
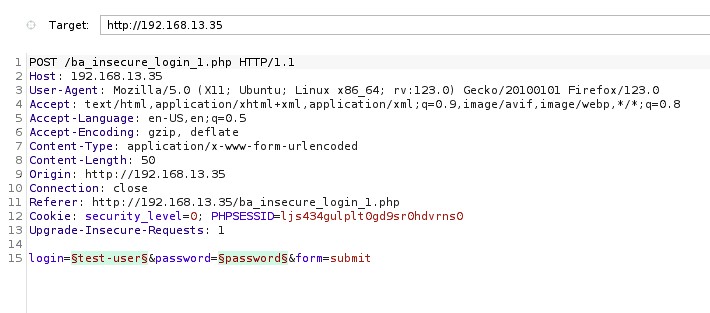


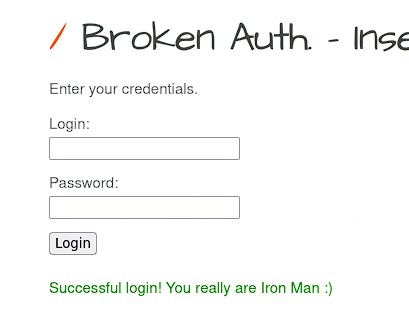
Write two or three sentences outlining mitigation strategies for this vulnerability:

| * applying Input validation to the system uses a process of checking user input to make sure it doesn't contain any special characters or commands that the server could run. * Clean up user input by encoding or removing any special characters that can be used for commands. * Prepared Statements are used When working with the operating system, use prepared statements to keep commands from being used on the system. |
| --- |

### Web Application 2: *A Brute Force to Be Reckoned With*

Provide a screenshot confirming that you successfully completed this exploit:



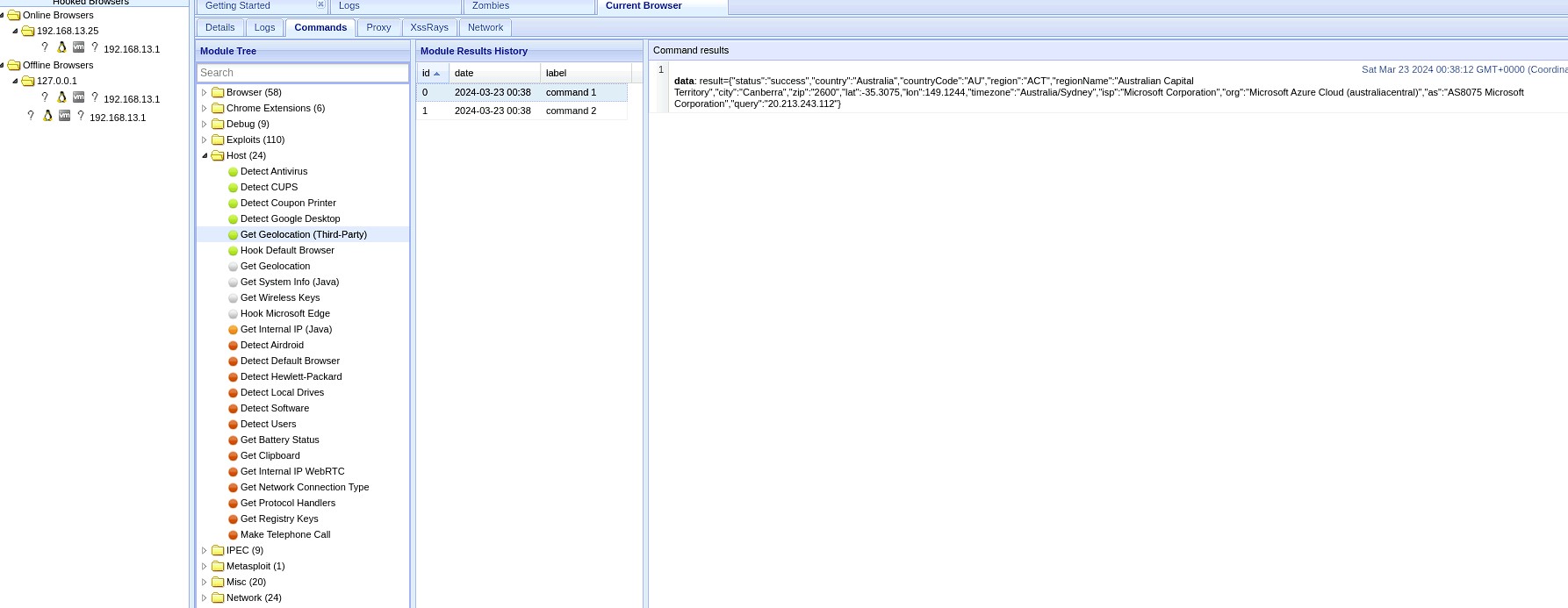
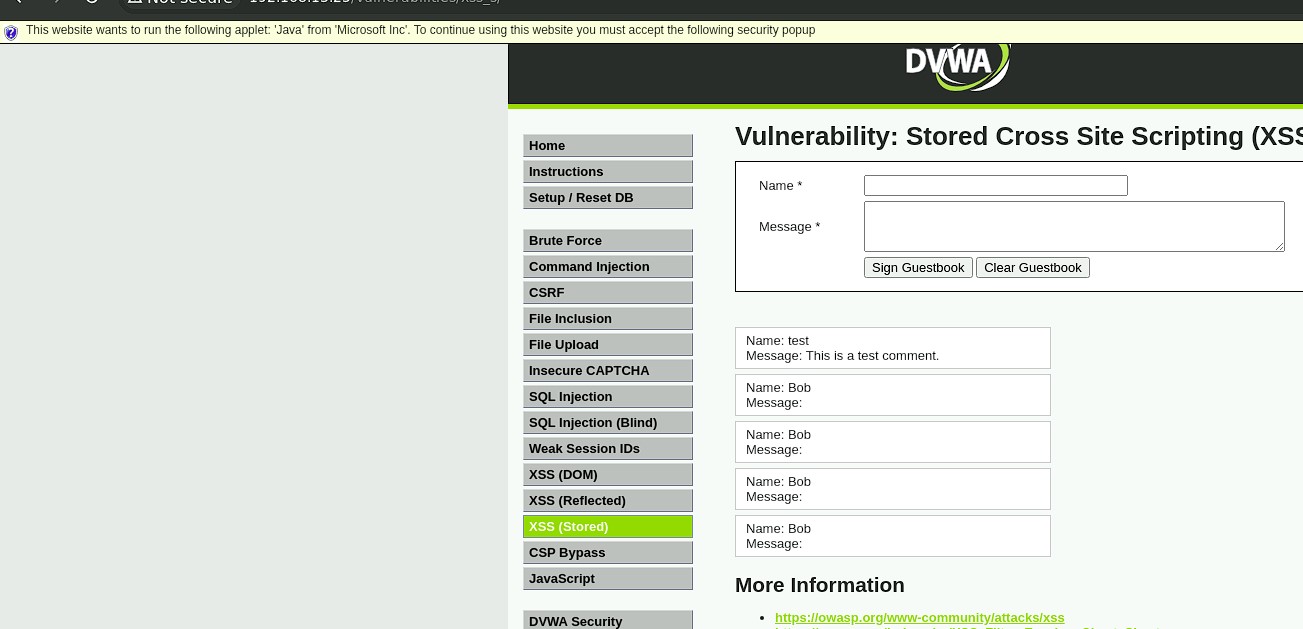
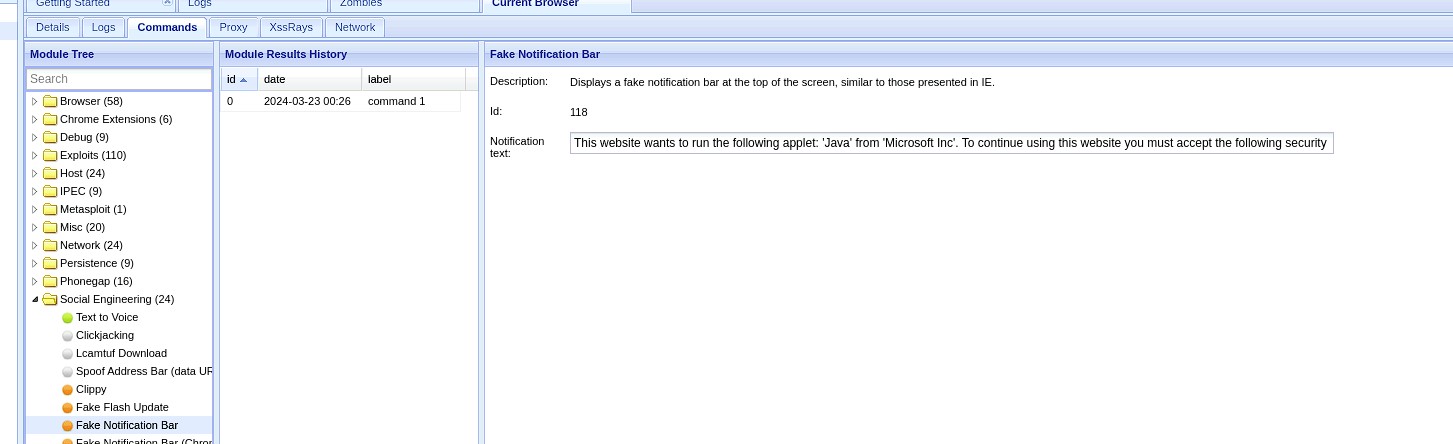
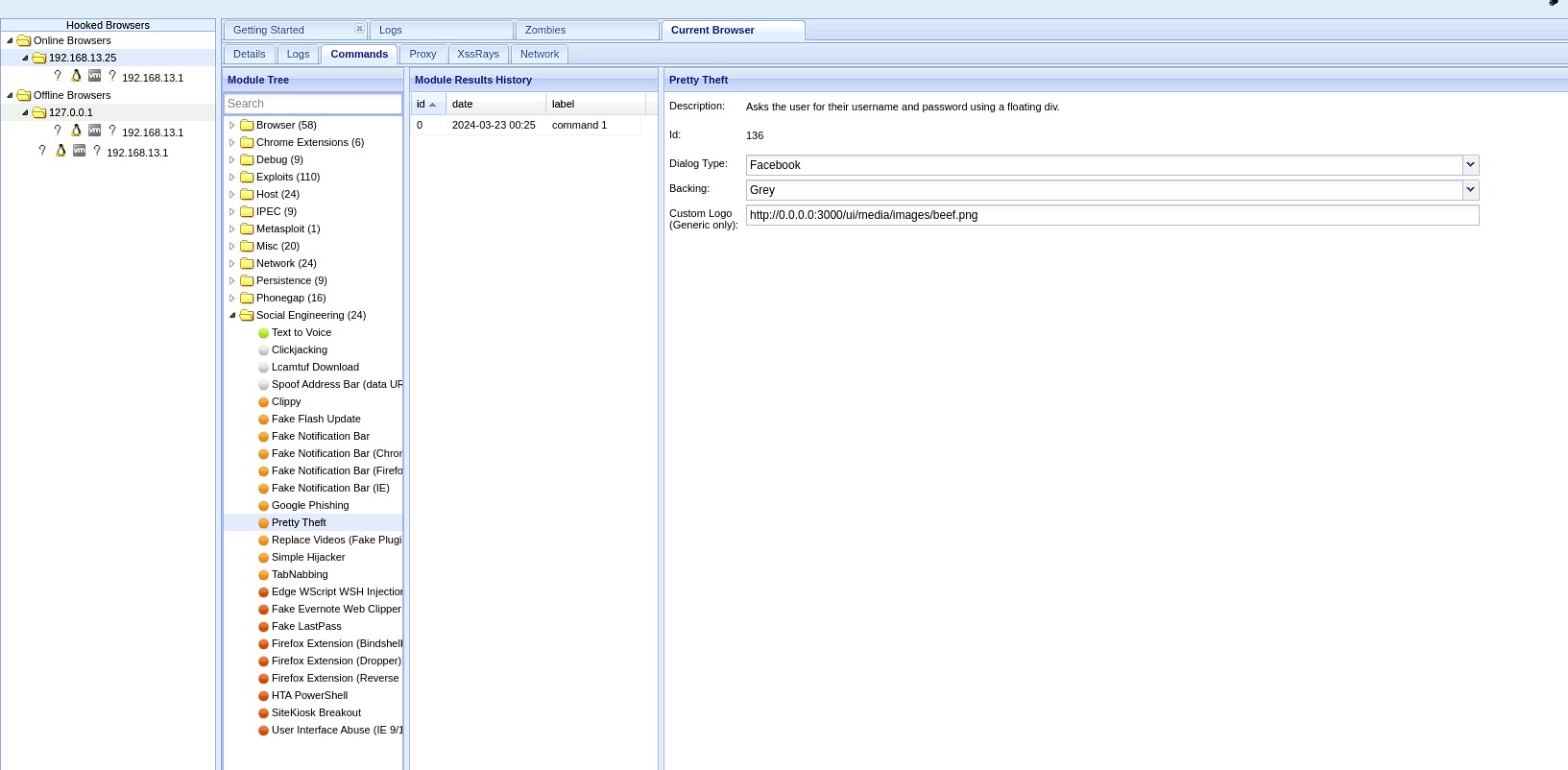
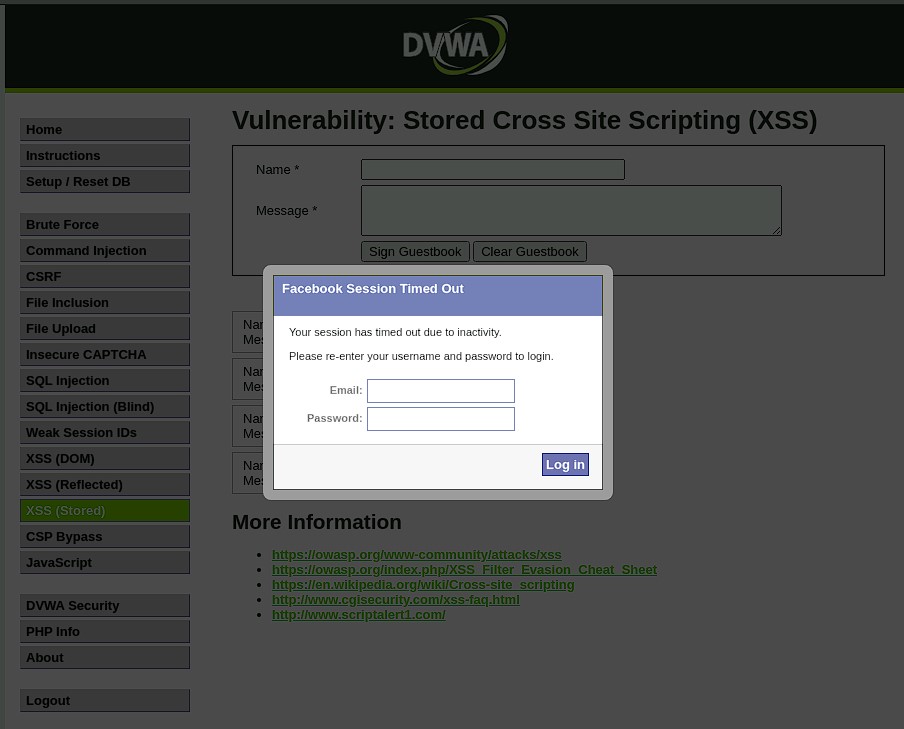
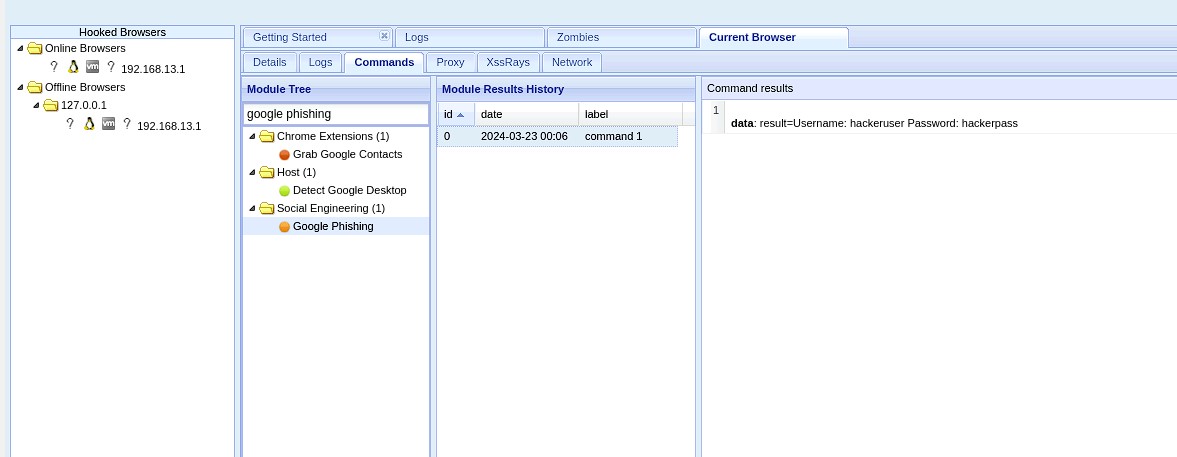


Write two or three sentences outlining mitigation strategies for this vulnerability:

| * Implement account lockout mechanisms to prevent multiple failed logins notify admins about locked accounts * Enforce strong password policies like Setting a minimum password length requirements.Prohibit the use of common or easily guessable passwords * Encourage regular password changes for administrators to change password every couple of months. * Monitor login attempts and unusual activity to detect and respond to brute force attacks monitor all logins attempts to develop a pattern. |
| --- |

### Web Application 3: *Where's the BeEF?*

Provide a screenshot confirming that you successfully completed this exploit:



Write two or three sentences outlining mitigation strategies for this vulnerability:

| * Sanitize input to remove or encode potentially malicious characters. * Encrypt data before rendering it in different formats. * Implement a Content Security Policy (CSP) to restrict sources from web pages that can load material. * Utilize input validation tools or frameworks for enforcing strict validation rules. * Use encoding functions provided by programming languages or frameworks to prevent XSS vulnerabilities. * Specify permitted sources for fonts, stylesheets, scripts, and other resources to enhance security. |
| --- |

* When you attempt to inject this payload, you will encounter a client-side limitation that will not allow you to enter the whole payload. You will need to find a way around this limitation.

I inspected the element and found it was at a maxlength if 50 i edited the html to a max length of 100

© 2023 edX Boot Camps LLC. Confidential and Proprietary. All Rights Reserved.